PERSEREC

Technical Report 17-07
June 2017

Improving Mental Health Reporting Practices in Between Personnel Security Investigations

Stephanie L. Jaros
Donna L. Tadle
David Ciani
Keith B. Senholzi, Ph.D.
Northrop Grumman Technology Services

Rene Dickerhoof, Ph.D.
Defense Personnel and Security Research Center
Office of People Analytics

OPA
OFFICE OF PEOPLE ANALYTICS

Approved for Public Distribution
Defense Personnel and Security Research Center
Office of People Analytics

Technical Report 17-07 **June 2017**

Improving Mental Health Reporting Practices in Between Personnel Security Investigations

Stephanie L. Jaros, Donna L. Tadle, David Ciani, Keith B. Senholzi, Ph.D.
Northrop Grumman Technology Services

Rene Dickerhoof, Ph.D., *Defense Personnel and Security Research Center/OPA*

Released by – Eric L. Lang, Ph.D.

Defense Personnel and Security Research Center
Office of People Analytics
400 Gigling Rd.
Seaside, CA 93955

REPORT DOCUMENTATION PAGE

REPORT DOCUMENTATION PAGE	**Form Approved OMB No. 0704-0188**

1. REPORT DATE:	2. REPORT TYPE Technical Report	3. DATES COVERED:
4. Improving Mental Health Reporting Practices in Between Personnel Security Investigations	5a. CONTRACT NUMBER:	
	5b. GRANT NUMBER:	
	5c. PROGRAM ELEMENT NUMBER:	
6. AUTHOR(S): Stephanie L. Jaros, Donna L. Tadle, David Ciani, Keith Senholzi, Ph.D., Rene Dickerhoof, Ph.D.	5d. PROJECT NUMBER:	
	5e. TASK NUMBER:	
	5f. WORK UNIT NUMBER:	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defense Personnel and Security Research Center Office of People Analytics 400 Gigling Road Seaside, CA 93955	8. PERFORMING ORGANIZATION REPORT NUMBER PERSEREC-TR-17-07	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITOR'S ACRONYM(S)	
	11. SPONSORING/MONITOR'S REPORT NUMBER(S):	

12. DISTRIBUTION/AVAILABILITY STATEMENT: (A)

13. SUPPLEMENTARY NOTES:

ABSTRACT: The purpose of the current study was to (1) provide an initial examination into mental health-related incident reporting trends and to (2) evaluate associated policy and reporting practices as they occur in the field. To this end, FY10-FY15 Joint Personnel Adjudication System (JPAS) incident reports were analyzed, mental health reporting policies were reviewed, and interviews with personnel security subject matter experts (SMEs) were conducted. Findings uncovered that approximately 6% of all incident reports pertained to Guideline I issues (as entered by security managers [SMs]). Further, the bulk of these incidents encompassed suicide attempts, suicidal ideation, and/or depression. Although the recently released DoD Manual 5200.02 (Procedures for the DoD PSP) now includes "suicide threats, attempts, or gestures or actions" as a specific reportable behavior, it is not clear how SMs should follow-up with subjects once these incident reports are established. Policy review and SME discussions underscore the need to further clarify mental health-related reporting requirements (generally) and to provide guidance to SMs and other involved parties about how best to help subjects when self-harm is a relevant concern. Recommendations are also made to clarify how local personnel security files should be maintained and/or shared across DoD's personnel security community and to begin tracking frequency and timeliness metrics for all incident reporting. Annual incident reporting metrics would help DoD better understand trends and gaps in both Guideline I and Non-Guideline I vetting procedures alike.

14. SUBJECT TERMS:

15. SECURITY CLASSIFICATION OF: UNCLASSIFIED			16. LIMITATION OF ABSTRACT:	17. NUMBER OF PAGES: 61	19a. NAME OF RESPONSIBLE PERSON: Eric L. Lang, Director
a. REPORT: UNCLASSIFIED	b. ABSTRACT: UNCLASSIFIED	c. THIS PAGE: UNCLASSIFIED			19b. TELEPHONE NUMBER (Include area code): 831-583-2846

REPORT DOCUMENTATION PAGE

PREFACE

A fair and effective Personnel Security Program (PSP) requires timely reports of, and responses to, issues of potential security concern that surface in between national security background investigations. The *Adjudicative Guidelines for Determining Eligibility to Classified Information* (1997; revised December 2005) outline such issues, but those listed under "Guideline I: Psychological Conditions" often are difficult to assess and pose unique challenges.

In response to a tasking from the Office of the Under Secretary of Defense for Intelligence (OUSD[I]), the Defense Personnel and Security Research Center (PERSEREC) analyzed mental health-related incident reports established in the Joint Personnel Adjudication System (JPAS), reviewed relevant policy, and interviewed personnel security subject matter experts (SMEs) to obtain a foundational understanding of the current reporting landscape. This report presents the results of these efforts and provides recommendations to improve the Department of Defense's mental health reporting process based on this information.

Eric L. Lang, Ph.D.
Director, PERSEREC

EXECUTIVE SUMMARY

National security background investigations are mandated to detect, deter, and prevent potential security concerns, but considerable time elapses in between the initial investigation and the periodic reinvestigation. In the interim, cleared Department of Defense (DoD) employees are required to report potential security concerns that pertain to self and others. Unlike the straightforward behaviors and clear thresholds associated with many guidelines (e.g., criminal arrests, financial issues), mental health issues that fall under "Guideline I: Psychological Conditions" (hereinafter, "Guideline I") pose unique and complex challenges to employees, security personnel, and adjudicators (Shedler & Lang, 2015).

The purpose of this report is to examine Guideline I-related incident reporting trends, mental health reporting policy, and associated personnel security procedures as they occur in the field. This work was then used to formulate recommendations to improve overall processes.

METHOD

Quantitative and qualitative methods were used to identify and assess mental health reporting processes across DoD. To begin, all security incidents reported between FY10 and FY15 were analyzed. Next, mental health reporting policies were reviewed, and finally, personnel security subject matter expert (SME) interviews were conducted.

INCIDENT REPORT FINDINGS

The Joint Personnel Adjudication System (JPAS) incident report analysis revealed the following:

- Security managers (SMs) established approximately 50,000 incident reports per year between FY10 and FY15. Of those, about 6% pertained to a Guideline I issue.
- Based on initial SM comments entered into JPAS, most Guideline I incidents reflected suicide attempts, suicidal ideation, and/or depression.
- SMs were more likely to suspend an employee's access when they established Guideline I incidents relative to Non-Guideline I incidents (31% vs. 25%, respectively). Analysis of SM comments/incident descriptions did not reveal a clear cause for this disparity.
- Guideline I incidents associated with an adjudicative outcome were considerably less likely to be favorable than were Non-Guideline I incidents (37% versus 55%, respectively). Those Guideline I incidents that were associated with a favorable adjudicative outcome were more likely to reference treatment in SM comments, whereas those that did

not result in a favorable outcome were more likely to reference violence.

- Ultimately, incident report analyses underscored the value of assessing frequency, timeliness, and outcome metrics to better understand the scope of both Guideline I and Non-Guideline I vetting procedures alike and to examine trends in these reporting practices over time. Examination of incident report data can help to identify where process improvements are needed.

POLICY & PROCEDURE RECOMMENDATIONS

Policy review and SME discussions with personnel working in the field provided the following suggestions:

- DoD should personalize training requirements by addressing what to specifically report and how to follow-up on highly sensitive mental health concerns (e.g., should suicide attempts and/or ideation be established in JPAS without assurances that subjects are routed to an appropriate support channel?).
- DoD should prioritize clarifications to personnel security reporting policies—specifically, DoD Instruction 5200.02 [2014] *Personnel Security Program* and the recently released DoD Manual 5200.02 [2017] *Procedures for the DoD Personnel Security Program*. Currently, personal judgment and professional experience substitute for specific reporting instructions, which can result in inconsistent practices across DoD.
- DoD should clarify SMs' primary priorities and responsibility. Is the scope of the SM role to protect national security and thereby maximize the amount of information routed to the DoD Consolidated Adjudications Facility (CAF) for review, or is it to continue to use discretion to keep DoD personnel in access without interruption?
- DoD should maximize available information by illuminating the purpose and use of local personnel security files (e.g., can background investigators access these files for periodic reinvestigations?). These locally maintained files often contain potential security concerns that are not established in JPAS due to SM and/or commander discretion.
- DoD should track and further investigate the timeliness of Guideline I incident resolution processes to determine where procedures can stall. A report documenting this and other related metrics would help DoD understand the drivers of this problem. Mental health-related information should be collected and acquired in a timely manner to ensure fairness to personnel under investigation. A timely report and review process should ultimately increase reporting confidence as well.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF TABLES IN APPENDICES

LIST OF FIGURES IN APPENDICES

INTRODUCTION

National security background investigations are in place to detect, deter, and prevent potential security concerns, but considerable time elapses in between initial investigations and periodic reinvestigations. In the interim, cleared Department of Defense (DoD) employees are required to report potential security concerns that pertain to self and others under the Continuous Evaluation Program (CEP).

A successful CEP relies on automated and ongoing use of relevant personnel security databases as well as employee, supervisor, and co-worker incident reporting. Behaviors that require follow-up are covered under the 13 *Adjudicative Guidelines for Determining Eligibility to Classified Information* (1997; revised December 2005 and June 2017; hereinafter, "adjudicative guidelines").

Unlike the straightforward behaviors and clear thresholds associated with many guidelines (e.g., criminal arrests, financial issues), mental health issues that fall under "Guideline I: Psychological Conditions" (hereinafter, "Guideline I") pose unique and complex challenges to the reporting and vetting process (Shedler & Lang, 2015). For example, considerable stigma continues to surround mental illness and psychological conditions, which is not likely to abate if DoD's Personnel Security Program (PSP) inappropriately penalizes personnel who seek treatment. Additionally, reliance on employee reports to determine whether a mental health issue adversely affects their eligibility or another employee's eligibility—a judgment that is difficult for trained mental health professionals—is inherently problematic. What follows is an effort to examine these issues with the goal of informing process improvements.

THE PRESENT STUDY

This study assesses DoD's mental health reporting process to identify and mitigate potential security concerns that arise in between security investigations. The purpose of this report is to examine Guideline I-related incident reporting trends, mental health reporting policy, and associated personnel security professional procedures that occur in the field. Specific study objectives include:

- Providing an overview of the number and type of Guideline I incidents reported in DoD's centralized system of record and evaluating associated events such as access suspensions and adjudication outcomes;
- Isolating and evaluating mental health reporting policies and procedures developed for use by DoD components;
- Conducting subject matter expert (SME) interviews to better understand obstacles and issues experienced by security managers (SMs) and other personnel security staff working in the field; and
- Reporting findings and empirically based recommendations to improve the current mental health reporting process.

METHOD

Quantitative and qualitative methods were used to examine and assess mental health reporting processes across the Department of Defense (DoD). To begin this work, all security incidents reported between FY10 and FY15 were analyzed. Lastly, mental health reporting policies were reviewed and interviews with personnel security subject matter experts (SMEs) were conducted to better understand how these vetting activities occur in the field.

ANALYSIS OF INCIDENT REPORTING

To examine incident reporting trends, data were obtained from the Joint Personnel Adjudication System (JPAS), DoD's system of record for personnel security determinations. JPAS contains initial and periodic security clearance data as well as incident reports provided by self, co-workers, and/or supervisors in between these investigations. JPAS also tracks the status of security clearances as well as other relevant investigation and adjudication information. For this effort, data associated with incident reports entered into JPAS between October 1, 2009 (FY10) and September 30, 2015 (FY15) were reviewed.

To begin the analyses, incident counts—as entered in JPAS by security managers (SMs)—were summarized with a focus on Guideline I (i.e., Psychological Conditions) versus Non-Guideline I-related issues (e.g., Personal Conduct, Foreign Influence). These data were first examined over time and across SM-selected adjudicative guidelines. Next, SM free text comments, provided at incident establishment, were analyzed to better understand the types of mental health concerns that ultimately make their way into JPAS. To do this, contextual differences between (1) Guideline I and Non-Guideline I-selected incidents, (2) Guideline I incidents with and without access suspensions, and (3) Guideline I incidents with 'favorable' and 'not favorable' adjudication outcomes were examined, a term weighting algorithm was applied (Salton & Buckley, 1988) to these data, and corresponding word clouds were developed.

Finally, after completing these content comparisons, Guideline I and Non-Guideline I incidents were also examined by SM access suspension (suspended/not suspended), adjudication timeliness (days to closing), and adjudication outcome (favorable/not favorable). Additionally, to understand and clearly illustrate the full JPAS incident reporting process from establishment through adjudication, two flow chart process diagrams were created. These diagrams illustrate the relative differences in incident counts, access suspensions, and adjudication outcomes between Guideline I and Non-Guideline I incidents. **Appendix A** provides a complete overview of the quantitative methods employed in this study.

ASSESSMENT OF POLICY & PROCEDURES

Relevant DoD policies and reports were gathered and reviewed to understand the mental health reporting environment within DoD. Executive-level policies along with DoD- and DoD-component level policies were first reviewed and a timeline of mental health considerations within DoD's Personnel Security Program (PSP) was created. When possible, the timeline highlighted guidance regarding mental health concerns specifically (e.g., Guideline I adjudicative issues). This chronological information was used to identify commonalities, best practices, and information gaps across sources and to ultimately prepare questions for SME interviews. **Appendix B** provides a summary of the policy review in conjunction with the timeline depicting these documents and related events (see Figures B-1 and B-2, respectively).

Between February 2016 and June 2016, SMs, security policy officials, and a DoD Consolidated Adjudications Facility (CAF) adjudicator were interviewed about personnel security reporting and response practices across DoD. Discussions focused specifically on how different DoD components identified, tracked, and responded to mental health issues that surfaced in between cleared employees' national security background investigations.

After beginning the policy review process, interview participants were identified via online searches for personnel security and/or mental health reporting policy experts and use of a convenience sample of known experts. The security and/or security policy offices of the Service branches, DoD agencies, and DoD field activities with publicly available personnel security policies were contacted first. When policies or names were not available online, the general telephone numbers for DoD security offices were contacted.

In total, 22 participants from all four Services (Air Force, Army, Navy, and Marine Corps), six Defense Agencies, five Field Activities, and the DoD CAF were interviewed. Most interviews were conducted via teleconference although three were in-person. One trained interviewer led each discussion while at least one other team member took field notes. All field notes were compiled, cleaned, and sent back to interview participants for review and final approval. One participant withdrew from the study because they did not have supervisory approval to participate in the interview at the time it was conducted. **Appendix C** provides the complete SME interview protocol.

Upon completion of all interviews, three researchers reviewed interview responses and discussed best practices and notable comments. These reviews were then combined into a final set of mental health reporting themes, which were ultimately used to construct recommendations for improving reporting procedures.

INCIDENT REPORT RESULTS

The following section summarizes the Joint Personnel Adjudication System (JPAS) data relevant to each stage of the incident reporting process, beginning with the establishment of incidents by security managers (SMs) through case close by adjudicators at the DoD Consolidated Adjudications Facility (CAF).

INCIDENT REPORT TRENDS, FY10–FY15

Between October 1, 2009 (FY10) and September 30, 2015 (FY15), DoD SMs and other authorized personnel established 295,674 unique incident reports in JPAS. Table 1 shows the number of entries for all Guideline I and Non-Guideline I incidents established in JPAS during this time period.

Table 1
Guideline I and Non-Guideline I Incidents Established by Fiscal Year, FY10–FY15

Fiscal Year	Guideline I	Non-Guideline I	Total
2010	2,410 (5%)	47,918 (95%)	50,328
2011	2,716 (5%)	47,993 (95%)	50,709
2012	2,966 (6%)	48,428 (94%)	51,394
2013	3,176 (6%)	47,935 (94%)	51,111
2014	3,908 (8%)	45,942 (92%)	49,850
2015	3,131 (7%)	39,151 (93%)	42,282
Total	18,307 (6%)	277,367 (94%)	295,674

Note. Guideline I vs. Non-Guideline I designations were based on how SMs entered incidents when they were established in JPAS (i.e., they were not determined by adjudicators).

As Table 1 indicates, approximately 50,000 incident reports were established in JPAS in a given fiscal year, and SMs categorized approximately six percent of these incidents under Guideline I concerns. The median number of days between the date a Guideline I incident occurred and/or was reported was 8. The median number of days between the date a Non-Guideline I incident occurred and/or was reported was 19.[1]

Figure 1 depicts these reporting trends over time and indicates that the total number of Guideline I incident reports steadily *increased* through FY14, but then began to decline in FY15. Conversely, Non-Guideline I incident reports generally *decreased* through FY14 and continued to decline in FY15.

[1] In some cases, an incident occurred on the same day a SM learned about it, but in other cases the incident preceded notification.

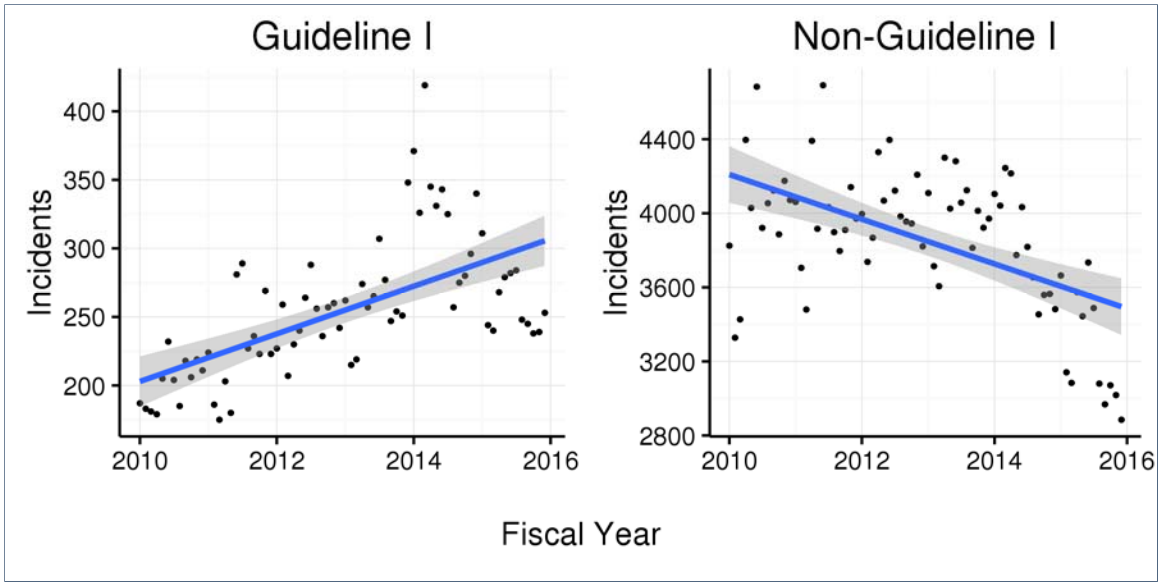

Figure 1 Guideline I versus Non-Guideline I Incidents Established by SMs per Month, FY10–FY15

ESTABLISHING AN INCIDENT REPORT

When SMs first establish an incident in JPAS they may select multiple adjudicative guidelines to categorize it. Table 2 shows the 459,999 adjudicative guidelines selected by SMs to classify the 295,674 incident reports established between FY10 and FY15.

Table 2
Adjudicative Guideline Selection by Security Managers, FY10–FY15

Guideline	Number of Incidents*	Percent of All Incidents (N = 295,674)
E Personal Conduct	149,090	50%
J Criminal Conduct	101,734	34%
H Drug Involvement	60,145	20%
G Alcohol Consumption	53,909	18%
F Financial Considerations	32,549	11%
I Psychological Conditions	18,307	6%
K Handling Protected Information	13,847	5%
D Sexual Behavior	11,868	4%
B Foreign Influence	6,111	2%
M Use of Information Technology Systems	4,994	2%
L Outside Activities	4,688	2%
C Foreign Preference	1,684	<1%
A Allegiance to the United States	1,073	<1%
Total	459,999	100%

*Incidents are not mutually exclusive.

INCIDENT REPORT RESULTS

Table 2 indicates that SMs categorized 50% of all incidents as Personal Conduct issues, which the adjudicative guidelines define broadly as conduct that suggests "untrustworthiness" or an "unwillingness to comply with rules and regulations." After Personal Conduct, SMs categorized 34% of all incidents under Criminal Conduct, followed by Drug Involvement (20%), and then Alcohol Consumption (18%). As previously noted, SMs categorized six percent of all incidents as relevant to Psychological Conditions.

Guideline I Incidents & Adjudication Guidelines

Of the 18,307 Guideline I incident reports established between FY10 and FY15, SMs categorized over half (55%) as Guideline I-*only* issues. That is, 10,126 of the 18,307 incident reports entered by SMs pertained solely to Psychological Conditions.

For the remaining 8,181 Guideline I incidents established between FY10 and FY15, SMs selected at least one other guideline in addition to Guideline I. In concurrence with the SM guideline selections shown in Table 2, SMs most commonly associated Guideline I incidents with Personal Conduct (n = 6,508), followed by Criminal Conduct (n = 2,492), Alcohol Consumption (n = 1,647), and then Drug Involvement (n = 1,078). The remaining eight adjudication guidelines were rarely associated with Guideline I incidents (i.e., fewer than 500 incidents per adjudication guideline).

Guideline I Incident Themes

In addition to examining incident counts by adjudication guidelines, researchers analyzed the free text comments entered by SMs at incident establishment in JPAS. Figure 2 presents these results in the form of two comparative word clouds. The size of each term in the word cloud is based on a term weighting algorithm referred to as a Term Frequency-Inverse Document Frequency (TF-IDF) score. A high TF-IDF ratio was achieved when a high term frequency (e.g., 'suicide') existed within SM comments but a low term frequency existed among combined comments (i.e., this weighting strategy filters out common words such as 'the,' 'it,' etc.).

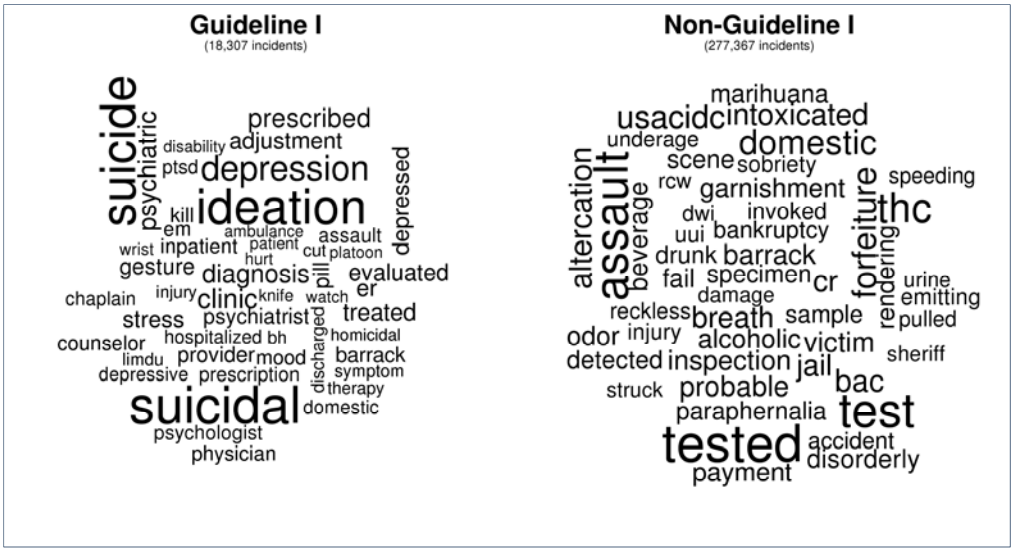

Figure 2 Guideline I versus Non-Guideline I Initial SM JPAS Comments

As Figure 2 indicates, "suicide," "suicidal," "ideation," and "depression" were most strongly associated with Guideline I incidents, whereas Non-Guideline I incidents referenced testing and assault (possibly for drug- and alcohol-related events, which also appeared in the Non-Guideline I word cloud). Results displayed in Table 3 list the 10 words from each word cloud with the highest TF-IDF scores.

Table 3
SM Comment Terms Associated with Guideline I vs. Non-Guideline I Incidents

Guideline I		Non-Guideline I	
Word	**TF-IDF Score**	**Word**	**TF-IDF Score**
Suicidal	0.48	Tested	0.34
Ideation	0.43	Test	0.29
Suicide	0.43	Assault	0.29
Depression	0.21	THC (Tetrahydrocannabinol)	0.23
Clinic	0.13	Domestic	0.16
Prescribed	0.12	Forfeiture	0.15
Diagnosis	0.11	USACIDC (U.S. Army Criminal Investigation Command)	0.13
Psychiatric	0.11	Altercation	0.12
ER (Emergency Room)	0.10	BAC (Blood Alcohol Content)	0.12
Treated	0.10	Intoxicated	0.12

Guideline I Incident Suspensions

SMs have the authority to suspend an employee's access to classified information when they establish an incident in JPAS. Following suspension, some DoD components can reassign an employee to a position that does not require access, but in many cases an employee is placed on administrative leave until the JPAS

incident is resolved. Table 4 shows the frequency of such access suspensions and indicates that, overall, incidents that involved Guideline I were slightly more likely than Non-Guideline I incidents to be associated with an initial access suspension (31% versus 25%, respectively).

Table 4
Guideline I versus Non-Guideline I Incidents by SM Access Suspension

	Not Suspended	Suspended	Total
Guideline I Incidents	12,558 (69%)	5,749 (31%)	18,307
Non-Guideline I Incidents	207,826 (75%)	69,541 (25%)	277,367
All Incidents	220,384 (75%)	75,290 (25%)	295,674

To complement Table 4, researchers again analyzed the free text comments that SMs entered when they established incidents in JPAS. This was done to identify any differences between Guideline I incidents that prompted an initial access suspension versus those that did not. Figure 3 presents these results in the form of two word clouds.

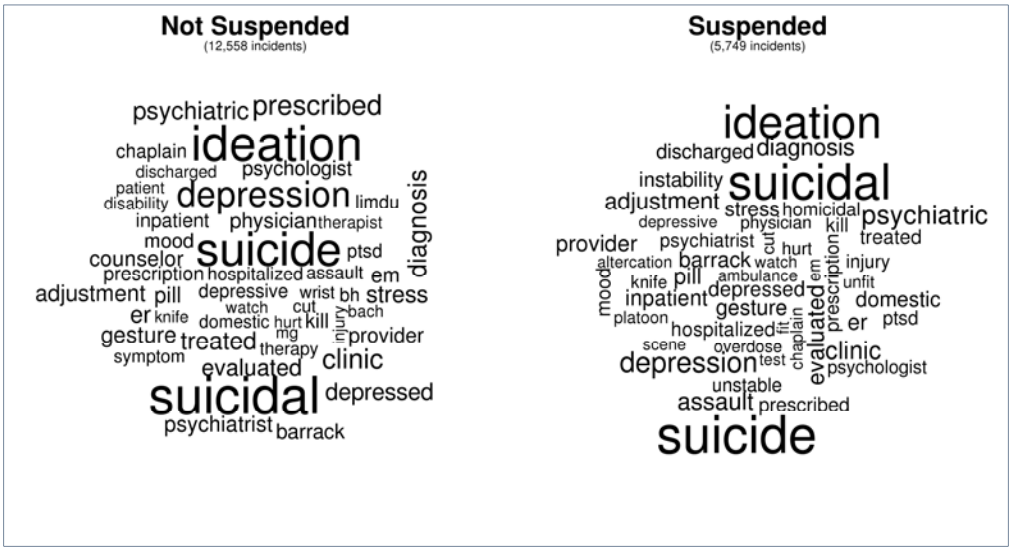

Figure 3 Guideline I SM Comment Terms Associated with Access Suspensions

As can be seen in Figure 3, the same four words—"suicidal," "ideation," " suicide," and "depression,"—are featured prominently in both word clouds, suggesting no discernable content differences between Guideline I incidents associated with access suspensions versus those that were not suspended. Table 5 lists the 10 words from each of these word clouds with the highest TF-IDF scores.

Table 5
Guideline I SM Comment Terms Associated with Access Suspensions

Not Suspended		Suspended	
Word	**TF-IDF Score**	**Word**	**TF-IDF Score**
Suicidal	0.48	Suicide	0.49
Ideation	0.44	Suicidal	0.45
Suicide	0.40	Ideation	0.38
Depression	0.23	Depression	0.15
Prescribed	0.14	Psychiatric	0.13
Clinic	0.13	Clinic	0.11
Diagnosis	0.12	Assault	0.10
Psychiatric	0.10	Adjustment	0.10
Treated	0.10	Diagnosis	0.10
ER (Emergency Room)	0.10	Evaluated	0.10

ADJUDICATING AN INCIDENT REPORT

After SMs establish incidents in JPAS, adjudicators at the DoD CAF determine if adjudication is required. If adjudication is not required, adjudicators may close the incident without further review. Specifically, adjudicators close incidents that are not deemed to present a national security concern (e.g., when a commander reports that his/her Soldier failed a written exam).

Table 6 summarizes the adjudication status of the 295,674 incidents established in JPAS between FY10 through FY15, including 29,116 incidents that were pending a decision at the time of data collection.[2]

Table 6
Guideline I versus Non-Guideline I Incidents by Adjudication Status

	Closed (no associated adjudication)	**Closed after Adjudication**	**Pending Decision**	**Total**
Guideline I Incidents	9,154 (50%)	6,627 (36%)	2,526 (14%)	18,307
Non-Guideline I Incidents	139,485 (50%)	111,292 (40%)	26,590 (10%)	277,367
All Incidents	148,639 (50%)	117,919 (40%)	29,116 (10%)	295,674

As indicated in Table 6, 50% of all closed JPAS incidents—whether Guideline I or Non-Guideline incidents—were not associated with an adjudicative outcome. This suggests that the DoD CAF was able to close half of all incident reports without requiring adjudication.[3] Slightly fewer closed Guideline I incidents were associated

[2] The 29,116 incidents pending at the time of data collection could be pending a decision of whether or not to refer for adjudication or pending an actual adjudication outcome.
[3] PERSEREC was not able to confirm the veracity of this interpretation prior to report finalization.

with an adjudicative outcome than were Non-Guideline I incidents (36% vs. 40%, respectively).

Adjudication Timeliness

Table 7 shows the median number of days between the date SMs established the incident in JPAS and the date DoD CAF closed the incident.

Table 7
Median Days Open in JPAS for Guideline I versus Non-Guideline I Incidents by DoD CAF Outcome

	Closed (no associated adjudication)	Closed after Adjudication	All Closed Incidents
Guideline I Incidents	197 days	170 days	183 days
Non-Guideline I Incidents	146 days	84 days	113 days
All Closed Incidents	149 days	89 days	118 days

Note. Table 7 includes the 148,639 closed incidents that were not associated with an adjudication outcome and the 117,919 incidents that were. It excludes the 29,116 incidents that were pending decision at the time of data collection.

Overall, Guideline I incidents stayed open longer than Non-Guideline I incidents, regardless of whether they were ultimately adjudicated (183 days versus 113 days, respectively). Perhaps counterintuitively, however, both Guideline I and Non-Guideline I incidents stayed open longer if they were not associated with an adjudication outcome. This result is discussed further in the Findings & Recommendations section of this report.

Adjudication Outcomes

When the DoD CAF refers an incident for adjudication, adjudicators review available documentation and either grant continued eligibility or proceed with due process in the absence of sufficient mitigating factors. Table 8 shows the adjudication outcomes for all 295,674 incidents established in JPAS between FY10 and FY15. For ease of reporting, researchers collapsed all possible adjudication outcomes into two categories: 'favorable' and 'not favorable'. **Appendix A** provides a complete list of the specific adjudication outcomes that were collapsed to create these two categories. Table 8 broadly shows that 148,639 closed incidents were not associated with an adjudication outcome, 64,218 resulted in a 'favorable' adjudication, 51,003 resulted in a 'not favorable' adjudication, 2,698 were associated with an adjudication outcome that could not be identified (missing data); and 29,116 were pending an outcome at the time of data collection.

Table 8
Guideline I versus Non-Guideline I Incidents by Adjudication Outcome

	Closed w/o Adjudication	Favorable	Not Favorable	Unknown Outcome	Pending Decision	Total
Guideline I Incidents	9,154	2,461	4,070	96	2,526	18,307
	(50%)	(13%)	(22%)	(1%)	(14%)	(100%)
Non-Guideline I Incidents	139,485	61,757	46,933	2,602	26,590	277,367
	(50%)	(22%)	(17%)	(1%)	(10%)	(100%)
Total	148,639	64,218	51,003	2,698	29,116	295,674
	(50%)	(22%)	(17%)	(1%)	(10%)	(100%)

Note. For a small number of incidents (*n* = 2,698; 'Unknown Outcome'), JPAS showed that cases were adjudicated and closed, but a 'favorable' or 'not favorable' outcome could not be determined due to missing data.

As indicated in Table 8, 22% of all 18,307 Guideline I incidents were not adjudicated favorably, in comparison to 17% of all 277,367 Non-Guideline I incident reports. This five-point difference widens considerably upon closer inspection. That is, when looking *only* at the subset of incidents that were referred for adjudication,[4] the point spread increases to 18%. In other words, Guideline I incidents referred for adjudication were considerably less likely to result in a favorable adjudication outcome than were Non-Guideline I incidents (37% versus 55%, respectively).

Researchers also analyzed SMs free text comments entered at incident reporting to identify any differences between Guideline I incidents that resulted in 'favorable' versus 'not favorable' adjudication outcomes. Figure 4 shows these results.

[4] Guideline I Favorable Outcome: 2,461/(2,461 + 4,070 + 96) = 37%
Non-Guideline I Favorable Outcome: 61,757/(61,757 + 46,933 + 2,602) = 55%

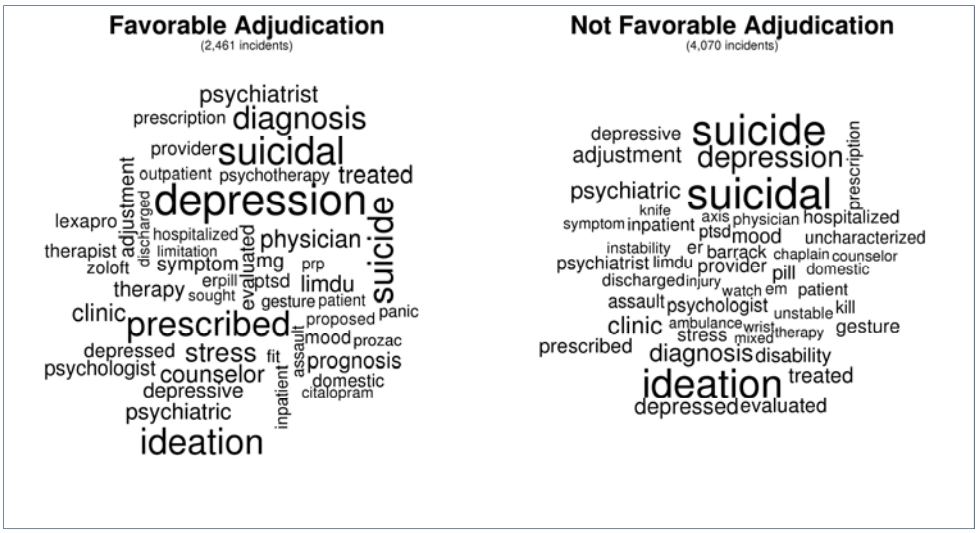

Figure 4 Guideline I SM Comment Terms Associated with Favorable versus Not Favorable Adjudication Outcomes

Regardless of adjudication outcome, Guideline I incidents commonly referenced suicide attempts and suicidal ideation. Notably, Guideline I incidents that were favorably adjudicated were more commonly associated with treatment, including visits to clinicians and medication management. Conversely, Guideline I incidents that were not favorably adjudicated were more frequently associated with violence (e.g., see terms "kill" and "knife"). Table 9 lists the 10 words from each of the word clouds with the highest TF-IDF scores.

Table 9
Guideline I SM Comment Terms Associated with Adjudication Outcome

Favorable		Not Favorable	
Word	**TF-IDF Score**	**Word**	**TF-IDF Score**
Depression	0.42	Suicidal	0.46
Suicidal	0.33	Suicide	0.45
Ideation	0.28	Ideation	0.39
Prescribed	0.28	Depression	0.21
Suicide	0.27	Clinic	0.14
Diagnosis	0.22	Diagnosis	0.14
Stress	0.16	Psychiatric	0.12
Clinic	0.13	Depressed	0.11
Physician	0.12	Adjustment	0.11
Counselor	0.12	Treated	0.10

OVERARCHING INCIDENT REPORTING PROCESS

Finally, Figure 5 summarizes the full JPAS incident report process, starting from when a SM established the incident in JPAS through DoD CAF's adjudication

outcome. The connections between the steps are sized according to the relative number of incidents that moved through them.

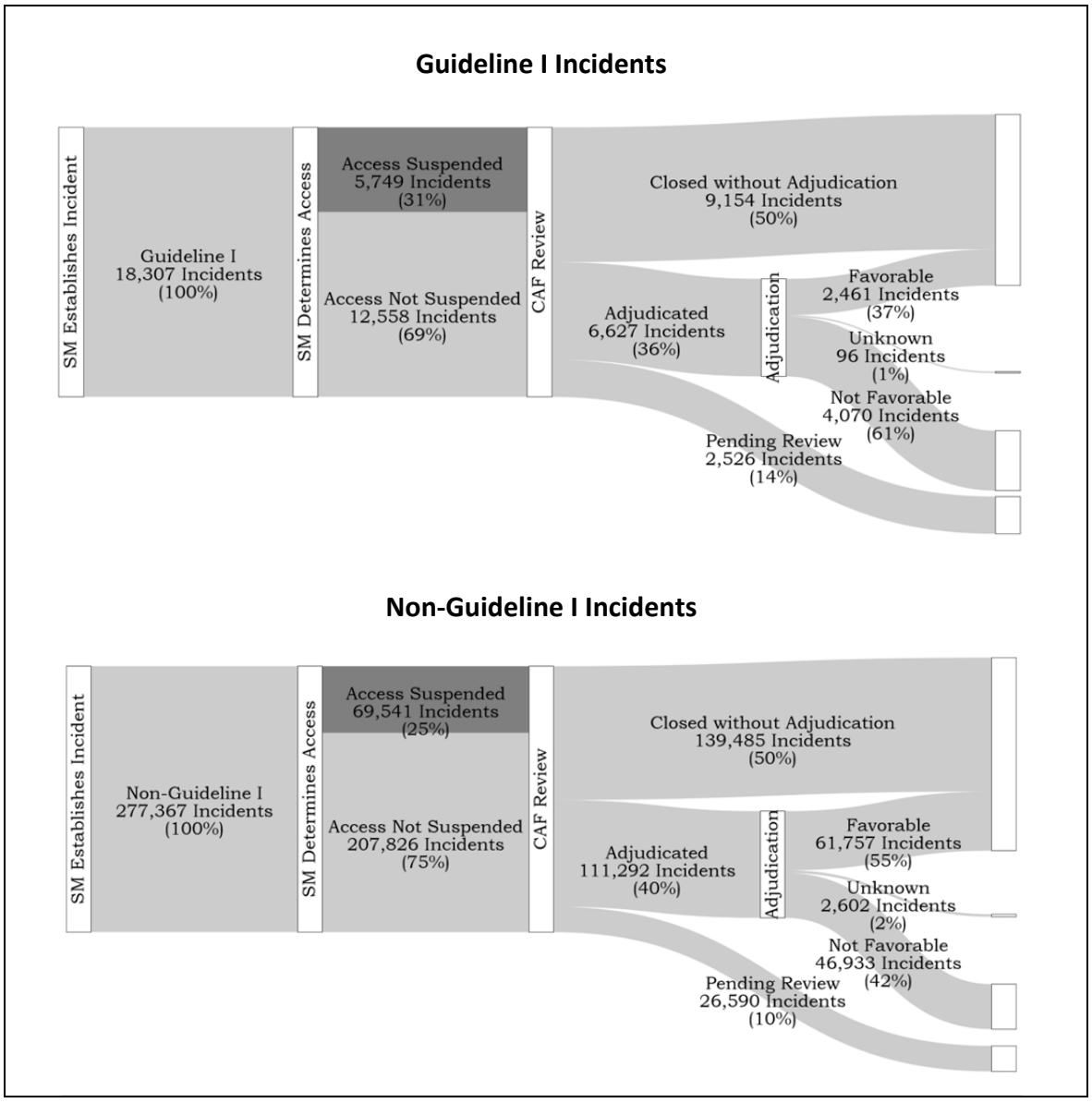

Figure 5 JPAS Overarching Incident Report Process, FY10–FY15

While the decision points depicted in Figure 5 may be straightforward, the decisions themselves and the corresponding justifications may not be. This point was reinforced during qualitative interviews with SMEs.

POLICY & PROCEDURE RESULTS

Researchers reviewed policy documents and interviewed personnel security subject matter experts (SMEs) to understand how the Joint Personnel Adjudication System (JPAS) incident process depicted in Figure 5 is operationalized in the field. In general, these interviews highlighted inconsistencies across the Department of Defense (DoD) components and communication challenges between components and the DoD Consolidated Adjudications Facility (CAF). What follows is a discussion of the major themes that emerged from the interviews along with representative SME quotations.

EMPLOYEE REPORTING REMAINS A CHALLENGE

Guideline I incidents accounted for six percent of all reports established in JPAS between FY10 and FY15 but, according to security managers (SMs), the number of mental health-related incidents should be higher. SMs believe that DoD personnel under-report mental health issues for at least two reasons. First, the criteria are unclear. One SM stated, “Training doesn’t provide a clear understanding of the signs of mental health defects versus someone who is just having a bad day.” Similarly, another SM shared a case in which a department knew about an employee’s bipolar disorder but did not notify the security office until the person went to the hospital. When the SM asked why the department had not reported the mental health concern earlier, he was told, “We weren’t sure if it was reportable.”

Second, in spite of DoD’s ongoing efforts to destigmatize mental health treatment, civilians and service members continue to fear that reporting on themselves or others will negatively impact careers. Several SMs agreed that employees worry they will lose their clearances, and possibly their jobs, if they report a mental health issue. As a result, “issues brew and brew.”

DISCRETION MAY BE UNAVOIDABLE

SMs do not establish JPAS incidents for every mental health report they receive from employees. Instead, two considerations guide their decision-making. First, as a practical matter, most SMs explained that not every mental health report warrants attention from DoD CAF. The findings depicted in Table 6 may support this statement—that is, half of all Guideline I incidents established and then closed in JPAS were not associated with an adjudication outcome.

SMs all agreed that Guideline I incidents that involved violence or the threat of violence to self or others must go into JPAS. Beyond these criteria, however, SMs relied on their professional judgment and experience to determine whether or not to establish a Guideline I incident in JPAS. For example, four SMs stated that they waited to establish a Guideline I incident in JPAS until a pattern of concerning behavior emerged, either because multiple people reported similar incidents or because an employee demonstrated the behavior multiple times. Other SMs relied

on Question 21 language in the SF-86 as their guide. For instance, one SM shared, "I would determine whether it needs to be elevated—issues associated with the Q21 carve-outs (i.e., counseling that resulted from grief, marital concerns, PTSD, or sexual assault) would not be elevated." Still other SMs required a mental health diagnosis to justify establishing an incident because, as one SM explained, "it's just a person saying he has an issue and there's no way to validate it."

Second, for all incident types, SMs hesitated to establish incidents in JPAS because of possible adverse consequences to the employee. SMs explained that open incidents signal—correctly or incorrectly—to other JPAS users that an employee had an issue serious enough to warrant review by an adjudicator. As a result, according to one SM, a JPAS incident, "may ruin a person's reputation or affect someone's job in a negative way." For example, an employee with an open JPAS incident report may fail to pass clearance, and as a result, be unable to attend important meetings and/or training sessions. Similarly, a person seeking employment with another Government agency may be denied a position because of an open JPAS incident report, even though it may eventually be mitigated. One SM also stated that any contractor with an open issue in JPAS is ineligible to support any contract within his/her component.

UNIQUE INFORMATION EXISTS OUTSIDE OF JPAS

JPAS is not the only system that SMs use to record mental health and other security-related concerns that arise in between employees' national security investigations. First, given the perceived severity and consequences of a JPAS incident, some SMs notified DoD CAF via the Consolidated Adjudications Tracking System (CATS) Portal rather than using JPAS. As one SM explained, "CATS is a notice to the CAF about information that doesn't necessarily warrant a big red flag in JPAS." This workaround, however, was not viewed as an acceptable practice to DoD CAF. An adjudicator explained, "If they added it to CATS but not the JPAS side, we'd want to make sure they added it to JPAS. That'd be our first action—letting them know they need to establish the incident [in JPAS]." Based on the interviews, however, SMs believed that they could bypass JPAS entirely.

Second, regardless of whether a SM chooses to establish an incident in JPAS or route material to DoD CAF via the CATS Portal, all SMs interviewed for this project said they maintained local personnel security files that included *all* employee reports. Some of these files were electronic, but many were hardcopy files that were neither easily searchable nor retrievable. Sometimes, SMs and Office of Personnel Management (OPM) investigators reviewed these files as part of an employee's periodic reinvestigation (PR). One SM explained, "Because the security office initiates the PR, the security office can look at [the] internal database to see if an individual has any prior issues." In other cases, however, SMs only shared information in response to a specific request by OPM investigators. Finally, one SM stated, "The security office is not allowed to release personnel security files to

investigators unless there's a court order and (in his experience), an investigator has never requested these files or more information on JPAS incidents."

RESOLUTION REQUIRES COLLABORATION

The SM's role in resolving an incident report is not finished after it is established in JPAS. The DoD CAF requires SMs to gather and submit all relevant documentation, and SMs, in turn, rely on employees, commands, and/or supervisors to prepare these materials, which are critical to the adjudication outcome. A DoD CAF adjudicator explained, "We don't want to send a Statement of Reasons (i.e., explanation of why the clearance was denied or revoked) and have to amend it when something changes."

The success of the incident resolution process, then, is contingent on relationships among stakeholders and the speed with which they submit information. According to a DoD CAF adjudicator, "The quality of the information is just not there sometimes. We tell them exactly what we need but we don't always get what we need in a timely fashion." Nevertheless, the adjudicator said that on average, most Guideline I reports are closed within 90 days. Table 7, however, shows that the median length of time for Guideline I incidents to be resolved was 183 days. In the meantime, employee incidents linger in JPAS, and the lengthy process may discourage future reporting.

FINDINGS & RECOMMENDATIONS

Taken together, the results of this research produced a multi-layered, comprehensive understanding of the mental health reporting environment within the Department of Defense (DoD). What follows is a summary of the major Joint Personnel Adjudications System (JPAS) findings from this project as well as the major recommendations identified from the policy and procedure data collection effort.

INCIDENT REPORT DATA

PERSEREC offers four broad findings, identified in the JPAS incident report data, which shed light on the scope of, and procedural outcomes associated with, Guideline I-related vetting:

- **Incident Report Trends:** Security managers (SMs) established approximately 50,000 incident reports per year between FY10 and FY15. Although Guideline I-specific incident reports increased in number over time, on average, about 6% of total incidents pertain to a Guideline I concern.
- **Incident Report Themes:** Initial SM comments entered into JPAS suggest that most Guideline I incidents reflect suicide attempts, suicidal ideation, and/or depression.
- **Security Manager Access Suspensions:** SMs are more likely to suspend an employee's access when they establish Guideline I incidents compared to Non-Guideline I incidents (31% vs. 25%, respectively). Analysis of incident descriptions did not reveal a clear cause for this disparity.
- **Adjudication Outcomes:** Guideline I incidents referred for adjudication were considerably less likely to result in a favorable adjudication outcome than were Non-Guideline I incidents (37% versus 55%, respectively). Those Guideline I incidents that were associated with a 'favorable' adjudicative outcome were more likely to reference treatment, whereas those that did not result in a favorable outcome were more likely to reference violence.

POLICY GUIDANCE & PROCEDURE FEEDBACK

PERSEREC offers five recommendations to improve the mental health reporting process based on review of relevant policy and discussions with security SMEs:

- **Personalize Training:** Given recently approved revisions to Question 21, which will apply a more targeted vetting approach, an increased emphasis will be placed on self, co-worker, and supervisor reporting of mental health issues of potential risk to national security. Training should stress reporting requirements and should address how to

follow-up on highly sensitive issues such as suicide attempts and/or ideation. For example, does DoD truly want these events to be in the purview of Guideline I incident reporting or should these cases instead be routed to Employee Assistance Programs (EAPs)? Perhaps a combination of these approaches could be applied to ensure both national security and subject protections. Reporting requirements and associated actions should be transparent to all personnel. Further, leadership should be empowered to personalize a DoD training template to meet local challenges, policies, and practices.

- **Clarify Policy Requirements:** DoD should prioritize clarifications to personnel security policies and procedural guidance, specifically DoD Instruction 5200.02 (2014) *Personnel Security Program* and DoD Manual 5200.02 (2017) *Procedures for the DoD Personnel Security Program*. Several SMs noted that DoD policies were "not accurate at all," "outdated," and/or lacked "clarity." Currently, personal judgment and professional experience substitute for clear policies, which contribute to inconsistent security practices across DoD.
- **Clarify Priorities & Responsibilities:** SMs are in a difficult position. They must establish rapport with employees and encourage them to report mental health issues, all the while knowing that these reports could lead to an employee's termination. DoD must clarify SMs' primary responsibility. Is the scope of the SM role to protect national security and thereby maximize the amount of information routed to the DoD CAF for review, or is it to use discretion to keep employees in access without interruption? If DoD prioritizes national security above all else, components must develop transparent, fair policies and processes to ensure they can meet mission requirements when employees temporarily move in and out of access. Given the revisions to Question 21 which are being implemented this year, there is an increased emphasis on self-reporting based on the individual's own perceptions of their mental health and whether their condition poses a national security risk, and the challenges faced by co-workers and security managers in the arena of under-reported security incidents.
- **Maximize Information:** DoD should maximize available information by illuminating the purpose and use of local personnel security files (e.g., can background investigators access these files for periodic reinvestigations?). These locally maintained files often contain potential security concerns that are not established in JPAS due to SM and/or commander discretion. Efforts to mitigate the risks of this stove-piped, restricted information should be considered.
- **Implement Frequency & Timeliness Metrics:** Many DoD CAF incident reports (Guideline I or other) require a considerable amount of information to close the case at hand. This information must be

collected and acquired in a timely manner to ensure fairness to personnel under evaluation. To establish a baseline understanding of the current length of these efforts, and to better track their duration over time, DoD should consider evaluating the frequency and timeliness of these practices on an annual basis. An annual record or report documenting such metrics would help DoD understand the drivers of this considerable workload and could potentially improve accountability efforts.

FUTURE CONSIDERATIONS

Finally, this project also gives rise to a number of questions for future research. These questions are outlined in the following list:

- What specific criteria are used to close Guideline I incidents that are note associated with an adjudication outcome? The answer(s) to this may identify and inform what specific mental health concerns constitute a reportable incident versus those that do not merit entry in the Joint Personnel Adjudication System (JPAS).
- How many suicide-related Guideline I incidents do not result in favorable adjudication outcomes? The answer to this may provide valuable guidance on whether suicide-related incidents should be established in JPAS or whether these cases should instead be worked through Employee Assistance Programs (EAPs).
- Why do closed incidents—Guideline I and Non-Guideline I—that are not associated with an adjudication outcome remain open longer in JPAS than those that are adjudicated? What guides a security manager's (SM's) decision to suspend and individual's access? These answers may ensure greater fairness within the incident reporting process.
- Once the Department of Defense Consolidated Adjudications Facility (DoD CAF) mitigates a security incident, it is up to the local SM to re-establish an employee's access if it was suspended. How long does this process take? Does the duration vary depending upon whether the individual is a service member, employee, or contractor? These questions also speak to issues of timeliness and fairness across the DoD's Personnel Security Program (PSP).

REFERENCES

DoD Instruction 5200.02 (2014) *Personnel Security Program*. Washington, DC: Author.

DoD Manual 5200.02 (2017) *Procedures of the Department of Defense Personnel Security Program*. Washington, DC: Author

ODNI Security Executive Agent Directive 4 (2017) *National Security Adjudicative Guidelines*. Washington, DC: Author.

Salton, G., & Buckley, C. (1988). Term-weighting approaches in automatic text retrieval. *Information Processing & Management*, *24*(5), 513-523.

Schmidt, M. (2008). The Sankey diagram in energy and material flow management. *Journal of Industrial Ecology*, *12*(1), 82-94.

Shedler, J., & Lang, E. L. (2015). *A relevant risk approach to mental health inquiries in question 21 of the questionnaire for national security positions (SF-86)* (15-01). Seaside, CA: Defense Personnel and Security Research Center.

APPENDIX A:

INCIDENT REPORT ANALYSES

FREQUENCY TABLES

The Joint Personnel Adjudication System (JPAS) dataset included every incident that security managers (SMs) established between October 1, 2009 (FY10) and September 30, 2015 (FY15). Variables included open and closure dates, the 13 adjudicative guidelines that SMs used to categorize incidents, access suspensions, and whether the Department of Defense Consolidated Adjudications Facility (DoD CAF) referred an incident for adjudication. For those incidents that the DoD CAF opened and subsequently adjudicated, variables included the adjudication outcome as well as a flag to indicate whether or not that outcome was considered 'favorable' or 'not favorable'.

JPAS data were restructured, as necessary, to enable analyses. First, the SM guideline(s) selected for each incident were converted from 13 independent true/false values into a separate table with one record for each selected guideline. Second, two new variables were calculated:

- Case Duration: Calculated as the number of days between when an incident opened and when it closed; and
- Incident Review Status: Calculated as whether or not the DoD CAF had completed its review process or not at the time of data collection.

WORD CLOUDS

Automated text analysis techniques were used to analyze free text comment fields provided by SMs at incident establishment.[5] First, extraneous punctuation, numeric figures, and a set of high frequency, low-information words known as "stop words" (e.g., and, the) were removed. Stop words were sourced from a pre-defined list included with the analysis software package. Second, any non-words (e.g., "XXXX") or words that identified specific security personnel and or base locations were removed.

Finally, Term-Frequency Inverse Document Frequency (TF-IDF) was used, which is an information retrieval technique designed to identify words most relevant to a specific document that is part of a larger collection of documents (Salton, 1988). In this case, each document was comprised of the initial comments provided by SMs for each incident that cited a given guideline (one document per guideline). Term Frequency (TF) is the number of times a term was used in a document divided by the total number of terms in that document. Inverse Document Frequency (IDF) is defined as the natural logarithm of the number of documents divided by the number of documents in which the term occurs. The TF-IDF score is the product of the TF and the IDF statistics.

[5] Researchers originally analyzed free text comments entered by both SMs and DoD CAF adjudicators, but comments from the latter group proved to be of limited value and were ultimately removed from these analyses.

Word clouds were developed to visualize the TF-IDF results. The relative sizes of the terms in the clouds correspond to their TF-IDF score. The figures were generated based on the 50 highest scoring terms.

ADJUDICATION OUTCOMES

For ease of reporting, all possible adjudication outcomes were collapsed into two categories: 'favorable' and 'not favorable'. Table A-1 includes the complete list of adjudication outcomes that were collapsed into these two categories using the JPAS Data Dictionary.

Table A-1
JPAS Data Dictionary Codes

Adjudicative Outcome	Favorable
LAA Confidential	Yes
Pending Reply to Statement of Reasons	Yes
Eligibility Administratively Withdrawn	No
Position of Trust	Yes
Ineligible for SCI	No
SCI Revoked	No
No Eligibility - Invest Reopened	Yes
Confidential	Yes
Denied	No
Interim Confidential	Yes
SCI Revoked - Ineligible for Eligibility	No
Secret - SCI Denied	No
Secret - SCI Revoked	No
No Determination Made	No
Eligible for SCI w/Waiver	Yes
Restricted to Nonsensitive Duties	No
Top Secret - SCI Revoked	No
Top Secret Only - SCI Ineligible	No
Interim Top Secret	Yes
Favorable	Yes
Revoked	No
Secret	Yes
Top Secret	Yes
Interim SCI	Yes
Top Secret - SCI Reqs Adjudication	Yes
Access Suspended	No
Loss of Jurisdiction	No
LAA Secret	Yes
SCI Denied	No

Adjudicative Outcome	Favorable
Eligibility Pending	No
Interim Secret	Yes
Action Pending	No
SCI - DCID 6/4	Yes
Interim Declination	No
Reinstatement Eligible	No

PROCESS FLOW DIAGRAM

To understand and illustrate the full JPAS incident report procedure from establishment to adjudication, various flow chart-type diagrams were researched and a Sankey network diagram (see Figure 5) was chosen to best represent the reporting process (Schmidt, 2008). Although originally developed for use in mechanical engineering and energy fields, in this project the Sankey diagrams show the volume of JPAS incidents flowing between the various steps in the reporting process for both Guideline I and Non-Guideline I incidents. Each of the “pipes” between the steps is scaled proportionately to the volume flowing through it. The advantage of this diagram over a simple flow chart is that it highlights the relative magnitudes of the applicable process outcomes.

APPENDIX B:

POLICY REVIEW

APPENDIX B

Various executive-level and federal policies guide the Federal Personnel Security Program (PSP), and in turn the Department of Defense (DoD) PSP. The DoD PSP has evolved over the years due to policy changes and security breaches that have driven program requirements. This appendix provides a brief historical overview of policies and events that have influenced DoD requirements, specifically for self, co-worker, and supervisor reporting of security-relevant mental health issues.

Early personnel security policy highlighted information considered relevant to determining whether one's employment in the federal government is consistent with national security. **Executive Order (EO) 10450, *Security Requirements for Government Employment* (1953, as amended [1])** references "any illness, including any mental condition of a nature which in the opinion of the competent medical authority may cause significant defect in the judgment or reliability of the employee." Though it states that this information would be collected in investigations, EO 10450 did not mention corresponding reporting requirements.

Early DoD forms used for investigations requested information deemed reportable for security purposes. **DoD Form 398-1 (DD398-1), *Statement of Personal History* (1962 [2])**, asked for basic personal information (e.g., full name, date of birth). Later revisions (**DD398, *Personnel Security Questionnaire,* 1981 [3]; DD398, 1990 [5]**) included a question pertaining to mental health—first, whether the individual had ever been a patient in a treatment facility—then, in the 1990 revision, whether the individual had ever been treated or counseled for a mental health condition.

Specific policy requiring employees to report security concerns about co-workers first appeared in the 1987 version of **DoD 5200.2-R, *Personnel Security Program* (1987 [4]; revised 1996 [8]); now DoD Manual 5200.02, *Procedures for the DoD's Personnel Security Program***. In the chapter, "Continuing Security Responsibilities", a brief section titled, "Coworker Responsibility" was provided, which charged co-workers with "an equal obligation [as the individual]" to report information of security concern regarding self or others with access to classified information. This version of DoD 5200.2-R included the same description of mental health-related information as EO 10450 in its list of reportable information.

EO 12968, *Access to Classified Information* (1995, as amended [6]), also instructed employees to report information that raised doubts as to whether another employee should be eligible to access classified information. Although the requirement did not reference the reporting of mental health concerns directly, it did note that no negative inferences concerning access eligibility standards should be made solely on the basis of receiving mental health counseling. In this same year (i.e., 1995), the **Standard Form (SF) 86 (revised [7])** replaced the DD398 as the personnel security reporting questionnaire. It required reporting of any consultations with health care professionals other than those specific to marital, family, or grief counseling, and not related to violence on an individual's part.

In 1997, the 13 adjudicative guidelines for determining one's eligibility to access classified information were established (***Adjudicative Guidelines for Determining Eligibility for Access to Classified Information*, 1997 [9]; revised 2005 [11]**). Guideline I, "Emotional, Mental, and Personality Disorders," included several disqualifying and mitigating conditions related to mental health issues. At the DoD-level, policies instructed individuals eligible to access classified information to report any and all personnel security concerns to their supervisor or security official; any behaviors or illnesses, to include mental conditions, were covered under these concerns (**DoD 5200.2-R, *Personnel Security Program,* 1987 [4]; revised 1996 [8]; DoDD, 5200.2, *DoD Personnel Security Program,* 1999 [10]**).

Policy in the mid to late 2000s sought to reduce stigma surrounding mental health counseling. Specifically, Guideline I was changed from "Emotional, Mental, and Personality Disorders" to "Psychological Conditions" and language within the Guideline was refined to encourage mental health treatment (***Adjudicative Guidelines for Access to Classified Information,* 1997 [9]; revised 2005 [11]**). In a report provided to Congress by the **DoD Task Force on Mental Health (2007 [12])**, recommendations were made to dispel stigma surrounding mental health treatment and to update DoD policy to reflect current knowledge about psychological health.

The SF-86 was again revised in 2007**[13]**; this time the question regarding mental health counseling (Question 21) asked about treatment and/or counseling for an emotional or mental condition, with exceptions for counseling that is "strictly marital, family or grief counseling, not related to violence by you." Various DoD memoranda were released emphasizing the importance of seeking mental health care when needed and pointing out that treatment seeking, by itself, cannot be the basis for denying someone a clearance (**DoD Memorandum, *Policy Implementation – Mental Health Question, Standard Form (SF) 86, Questionnaire for National Security Positions* [2008]; DoD Memorandum, *Mental Health Counseling and Treatment and Security Clearances* [2009]; DoD Memorandum, *Department of Defense Guidance on Question 21, Standard Form 86, Questionnaire for National Security Positions* [2012]**)[6]. Question 21 of the SF-86 was revised again in 2008 **[15]**. A note was added stating that mental health counseling alone does not serve as a reason to revoke or deny a clearance. Additionally, another exception—this one pertaining to reporting detailed information—was added for counseling related to adjustments to combat environments.

Around the same time, major efforts were made to outline responsibilities and to standardize policies pertaining to personnel security. In 2008, **EO 13647, *Reforming Processes Related to Suitability for Government Employment*,**

[6] These memoranda are not depicted in the policy timeline due to space constraints (Figures B-1 and B-2).

Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information **[14]**, designated the Director of National Intelligence (DNI) as the Security Executive Agent. As such, DNI was charged with developing standard and consistent policies and processes governing the federal government's personnel security program. With **Security Executive Agent Directive (SEAD) 1**, ***Security Executive Agent Authorities and Responsibilities*** **(2012 [21])**, the DNI established roles and responsibilities in the development, implementation, and oversight of the federal government's personnel security program, to include investigations, reinvestigations, and adjudications for determining access to classified information.

Regarding policy guidance, the DoD Inspector General (IG) reviewed security (e.g., physical, information, personnel) policy and guidance across DoD and spoke with those responsible for security policy development and implementation. The review found that the Department had many security policies that were redundant, incomplete, or inconsistent. Without consolidation of guidance or an overarching security policy, persons in the field had difficulties in complying with the various policies, which at times were outdated and unclear (**DoD IG Report: Assessment of Security Within the Department of Defense – Security Policy, 2012 [22]**).

The **2009 Fort Hood shooting [16]** and the **2010 WikiLeaks [18]** release resulted in a large-scale review of the federal government's PSP. Additionally, concerns regarding the mental stability of the perpetrators of these incidents prompted a re-evaluation of how best to capture relevant mental health information and provide better mental health care to DoD personnel (**"Protecting the Force: Lessons from Fort Hood" – Report of the DoD Independent Review, 2010 [17]; SF86, 2010 version [19]; DoDI 6490.08, *Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Service Members*, 2011 [20]**).

The **2013 mass shooting at the Washington Navy Yard [23]** led to more rigorous reviews of DoD's clearance granting procedures and how it handles mental health issues. After action reports highlighted how the perpetrator's employer and peers did not properly report behaviors indicative of emotional instability, and that if they had, the shooter would not have been granted his clearance (**"DoD Internal Review of the Washington Navy Yard Shooting: A Report to the Secretary of Defense", 2013 [24]; "Slipping Through the Cracks: How the D.C. Navy Yard Shooting Exposes Flaws in the Federal Security Clearance Process", 2014 [26]**). The reports provided recommendations such as revising Question 21 to take a risk-relevant approach by listing specific clinical conditions that are security risks; updating the Guideline I to specify clinical conditions of security concern; holding security personnel accountable for incident reporting; creating policy that would aid investigators to better collect mental health information; and updating and standardizing security education and training to identify reportable behaviors of security concern.

The Washington Navy Yard Shooting also prompted an Office of Management and Budget (OMB) review of policy regarding the granting of security clearances across the federal government. The findings were published in **"Suitability and Security Processes Review Report to the President" (2014 [25])**, which called for clearer guidance on reporting by both self and peers. The review made note that mental health issues "pose a unique reporting challenge" and federal efforts should be made "to address this complex issue with sensitivity." It also recommended revisions to the SF-86 to "focus on mental illness to the extent that it may impact an individual's judgment, reliability, and trustworthiness." Lastly, the review proposed a working group comprised of representatives from various federal agencies to "further examine the relevant intersection of mental health issues and suitability and security reporting."

Personnel policy since the 2014 review has emphasized peer reporting and clarified the types of mental health-related behavior that could be of potential security concern. For example, **DoDI 5200.02, *DoD Personnel Security Program (PSP)* (2014 [27])** indicates that no negative inference shall be raised solely on the basis of mental health counseling, though it may justify further inquiry if relevant to national security concerns. DoD 5200.2-R, currently being redrafted, charges individuals with access to classified information to report information of security concern (to include mental conditions, illnesses, or behaviors) on self or co-workers. DoD Manual (DoDM) 5200.02, Procedures for the DoD Personnel Security Program (currently being drafted), intended to replace DoD 5200.2-R, specifies negative suitability actions for those who fail to report such information on self or others. It also specifies reportable behaviors related to mental health (e.g., "erratic or unstable behavior indicating possible mental health issues"). As DoD 5200.2-R and the associated manual are not finalized documents, they are not depicted in the policy timeline shown in Figures B-1 and B-2.

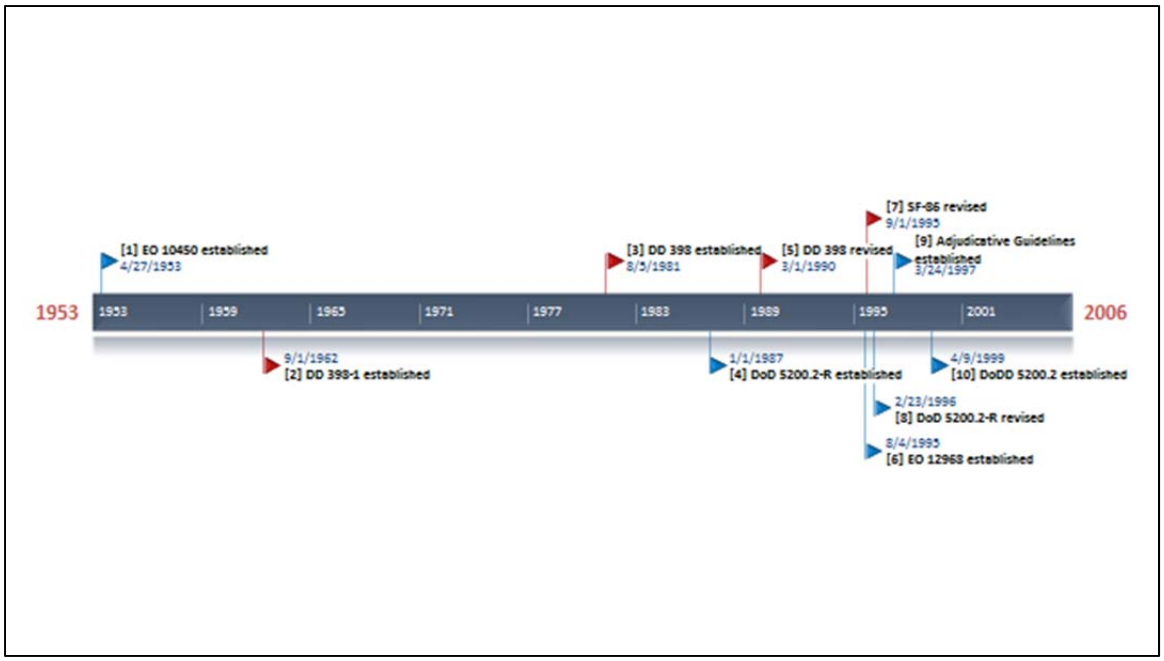

Figure B-1 Policy and Event Timeline (FY1953–FY2005)
Blue markers denote policy establishment and report releases. Red markers denote events and form revisions.

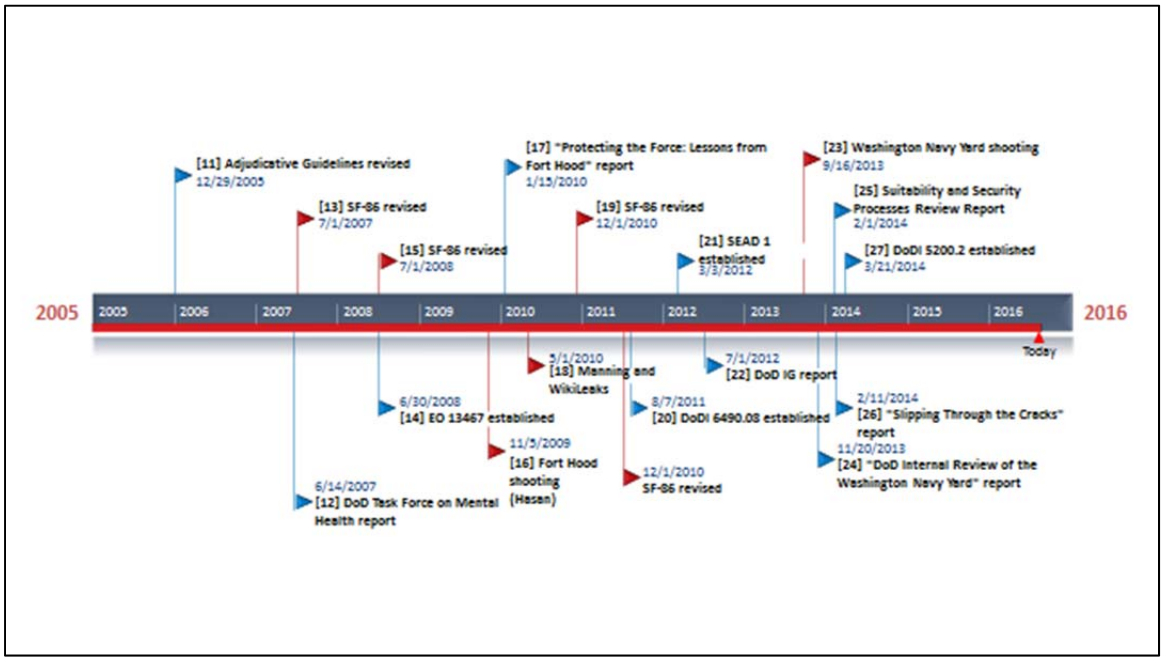

Figure B-2 Policy and Event Timeline (FY2005–Present)
Blue markers denote policy establishment and report releases. Red markers denote events and form revisions.

APPENDIX C:

INTERVIEW PROTOCOL

INTRODUCTION

Good morning/afternoon. As mentioned in our invitation email, this project is sponsored by OUSDI and the purpose is to identify personnel security policies and processes currently in place to detect and respond to mental health issues that arise in-between national security investigations (i.e., in-between initial and re-investigations for cleared populations).

The results will be published in a publicly available report. Individual feedback will be reported in the aggregate, but we will link agency names to policies and procedures that contain best practices for this challenging issue. Discussions with those involved in the personnel security process—with people like you—are the cornerstone of this study.

As a reminder, we expect the call today to take about 45 minutes to an hour of your time. To ensure that the research team gathers consistent information, we have a set of questions to guide the discussion but we can discuss other topics or issues as we go. If there are topics you don't feel you can or want to address please let me know and we'll move on.

What questions do you have before we get started?

SERVICE OVERVIEW

Before we talk about policies, we'd like to make sure we understand [the COMPONENT NAME].

(1) What percentage of your workforce has a national security clearance? What type of clearances do people typically have (e.g., Secret, Top Secret, TS/SCI, SAP, etc.)?

(2) Does [the COMPONENT NAME] have components that are a member of the intelligence community?

   (a) [IF NOT AN IC] Some organizations have applicants complete a national security investigation but they are not adjudicated until the person has a specific need for the clearance. Is this the case in your component?

   (b) [IF NOT AN IC] Some organizations give employees clearances but they are not given any accesses, including computer accounts or SCIF access, until a specific need comes up. Is this the case in your component?

(3) What system of record does your personnel security division use to record any kind of security-related incident? JPAS – for Secret and Top Secret? Scattered Castles – for TS/SCI?

POLICY REVIEW

Moving on to policies, we would like to start with the big picture. We want to confirm that we've identified the major executive-level and DoD-level policies that address personnel security reporting requirements in general and mental health reporting specifically. The major executive and DoD-level references we believe to be central to this topic are:

Table C-1
Key Reporting Authorities and Mental Health-related Guidelines

Source	Description	Relevant Statements (for Interviewer reference as needed)
EO12968 (1995) Access to Classified Information	Establishes a uniform Federal security program for employees who will be considered for initial or continued access to classified information.	PART 3-ACCESS ELIGIBILITY STANDARDS Sec. 3.1 Standards (e) **No negative inference concerning the standards in this section may be raised solely on the basis of mental health counseling.** Such counseling can be a positive factor in eligibility determinations. However, mental health counseling, where relevant to the adjudication of access to classified information, may justify further inquiry to determine whether the standards of subsection (b) of this section are satisfied, and mental health may be considered where it directly relates to those standards. PART 6-IMPLEMENTATION Sec. 6.2 Employee Responsibilities (b) **Employees are encouraged and expected to report** any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security.
DoDI 5200.02 (2014) Personnel Security Program (PSP)	Establishes policy, assigns responsibilities, and prescribes procedures for the DoD PSP (was a directive from 1999 that authorized DoD 5200.2-R).	Sec. 3. Policy (d) **No negative inference may be raised solely on the basis of mental health counseling.** Such counseling may be a positive factor that, by itself, shall not jeopardize the rendering of eligibility determinations or temporary eligibility for access to national security information. However, mental health counseling, where relevant to adjudication for a national security position, may justify further inquiry to assess risk factors that may be relevant to the DoD PSP. ENCLOSURE 2: Responsibilities Sec. 6 **The Heads of the DoD Components shall** (c) **Enforce requirements for prompt reporting of significant derogatory information**, unfavorable administrative actions, and adverse actions to the appropriate personnel security, human resources, and counterintelligence official(s), as appropriate, within their respective Component.
DoDM 5200.02 (2017) Procedures for the DoD Personnel Security Program (PSP)	Implements policy, assigns responsibilities, and provides procedures for the DoD PSP (was previously DoD 5200.2-R, 1987, 1996)	Sec. 11 CE and Reporting Requirements 11.1 General (c4) **Information that suggests an individual may have an emotional, mental, or personality condition that can impair judgment, reliability, or trustworthiness will be reported to** the supporting adjudication facility. Such information may include, but is not limited to: (a) A known history of a mental disorder; (b) A report that an individual has sought treatment for a mental, emotional, or substance abuse condition (commensurate with any reporting limitations of Section 21 on the SF86); (c) Direct and indirect threats of violence; (d) Physical altercations, assaults, or significant destruction of U.S. Government property; (e) An abrupt and significant change in an individual's appearance or behavior suggesting impaired judgment or stability (e.g., deteriorating physical appearance or self-care, social withdrawal); (f) Signs of substance use or intoxication on the job; (g) An indication of substance abuse after completion of treatment; (h) Evidence of alcohol or drug related behavior outside the workplace (e.g., driving under the influence, public intoxication charges); (i) Suicide threats, attempts, or gestures or actions; and (j) Any other behaviors which appear to be abnormal and indicate impaired judgment, reliability, or maturity.

Is this list exhaustive? What other executive and DoD-level policies have guided personnel security policies at [the COMPONENT NAME]? (List as provided and provide brief descriptions of the nexus to personnel security.)

(4) Now let's talk more specifically about reporting requirements. Thinking just about [the COMPONENT NAME]:

(a) I found the following policies that reference personnel security reporting requirements on your website:

[IF POLICIES EXIST] Why were these policies put in place? Was there something that [the COMPONENT NAME] wanted to put in place or emphasize that wasn't already in the higher-order policies we talked about?

[IF APPLICABLE] Do these policies apply to your entire workforce or only to your cleared workforce?

(5) What additional policies are in place at [the COMPONENT NAME] that you believe are relevant to our project? Would you be able to provide me with a copy of these policies?

(6) To summarize, at [the COMPONENT NAME], cleared personnel are required by policy to report the following to personnel security (develop list during discussion):

PROCESS

Now that I understand the policies and procedures in place at [the COMPONENT NAME], let's talk about how they work on a day-to-day basis.

(1) Let's say I work with you as part of [the COMPONENT NAME]. I am in between security investigations and begin to experience mental health issues that might affect my ability to hold a clearance. Walk me through the reporting process if I want to report my own information – starting with what I might have to report and then how I might make a report.

In your opinion, what would make a mental health issue reportable to personnel security?

How can I report my mental health issues? Via telephone hotline? Email? To my supervisor who will turn it in to personnel security?

What information will I need to provide?

Who will find out about my report? My supervisor? What temporary records are kept? What permanent records are kept?

(2) What about if my supervisor or co-worker has a concern about me. Does this change the process we just talked about? Are proxy reporters offered confidentiality?

(3) Once I make my report, what happens next?

What criteria are used to determine whether an issue is elevated? Who might receive the information next?

At any point is a medical expert consulted to determine whether a mental health issue has personnel security implications? If so, how does that factor into the reporting process?

Would my doctor be contacted or would a government doctor be contacted to review my information?

If the information was obtained by proxy, is the reporting party interviewed?

If the information was obtained by proxy, at what point is the subject of the report notified?

(4) Let's discuss how a mental health issue is resolved.

In the short-term, what must be done for a case to be closed by [the COMPONENT NAME]?

Is this information stored locally at [the COMPONENT NAME] for future retention?

Does the information become part of an individual's personnel security file? Is this information revisited during the person's PRI?

Is the information entered into JPAS?

What is your understanding of what happens once an incident has been logged into JPAS?

(5) Can you provide some examples of actual mental health concerns that have been reported to personnel security?

(6) Does [the COMPONENT NAME] keep aggregate records on the following:

- How often individuals make personnel security reports?
- Types of issues reported?
- The source of the report?

[IF AGGREGATE RECORDS ARE KEPT] Where is this information stored?

- If data are maintained, is it possible for us to review and/or report on de-identified trends to gain a greater understanding of reporting prevalence?

[IF NO RECORDS ARE KEPT] What is your general impression as to how frequently personnel security issues are reported? What about mental health issues specifically?

- Types of personnel security issues?
- Sources of personnel security issues?

EDUCATION & AWARENESS

(1) In general, what training do cleared employees receive regarding reporting requirements for personnel security? How often? Online or in-person?

(2) Is additional training required of supervisors/commanders? How often? Online or in-person?

(3) Either as part of the training listed earlier or as part of other trainings, what mental health behaviors are employees trained to identify and report?

(4) Sometimes the organization enables reporting behavior and sometimes it makes reporting more difficult.

What about [the COMPONENT NAME] increases the likelihood that employees will report mental health issues?

What about [the COMPONENT NAME] makes it less likely that employees will report mental health issues?

What do you think can be done to increase employee reports of mental health issues?

CONCLUSION

(1) Who else in your agency should I talk with about these issues? Would it be okay if I used your name in the invitation email?

Contact No. 1
Name and Position Title:
Phone Number:
E-mail Address:
_____

Contact No. 2
Name and Position Title:
Phone Number:
E-mail Address:
_____

Contact No. 3

Name and Position Title:

Phone Number:

E-mail Address:

(2) What organizations – in or outside DoD or even the federal government – stand out to you as having some of the best practices for personnel security reporting? Do you have any contacts there?

(3) What haven't we discussed that you think is important to the issue of mental health reporting? What didn't we ask?